UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- -x

UNITED STATES OF AMERICA	:	**SEALED INDICTMENT**
-v.-	:	
		S1 09 Cr. 1093
NIKOLAY NASENKOV and ALEKSANDR KALININ,	:	
Defendants.	:	

- -x

COUNT ONE

(Conspiracy to Commit Bank Fraud)

The Grand Jury charges:

THE DEFENDANTS

1. NIKOLAY NASENKOV, the defendant, was a computer hacker who resided in the vicinity of Moscow, Russia. As set forth more fully below, NASENKOV stole customer account data from various banks through hacking, and obtained additional misappropriated bank customer account data that ALEKSANDR KALININ, the defendant, had separately stolen through hacking.

2. ALEKSANDR KALININ, the defendant, was a computer hacker who resided in the vicinity of St. Petersburg, Russia. Among other things, KALININ stole data for customers' accounts at a bank through hacking, and made that information available to NIKOLAY NASENKOV, the defendant.

3. After obtaining account data, NIKOLAY NASENKOV, the defendant, distributed that stolen information to co-conspirators not named as defendants herein, who would, among

other things, use it to fraudulently encode and create cards to access automated teller machines ("ATMs"), thereby permitting those co-conspirators to withdraw millions of dollars in cash from victims' compromised bank accounts in New York, New York and around the world. NASENKOV also arranged for the bulk of this money to be sent to NASENKOV in Russia.

BACKGROUND

4. ATMs are computerized devices which, among other things, allow customers of banks to access their accounts, withdraw cash, and perform other activities, such as transferring funds and obtaining account balances, by inserting into the ATM a plastic card (an "ATM card") and entering a personal identification number ("PIN"). ATMs are commonly found in locations worldwide. There are numerous ATMs located in and around the New York City area.

5. ATM cards typically bear a magnetic stripe on which account-related information has been electronically encoded.

6. The information encoded on an ATM card's magnetic stripe includes, among other things, the customer identification number ("CIN") and a card verification value ("CVV"). The CIN is the unique number embossed or printed on the front of the ATM card. The CVV is a security feature which helps authenticate the ATM Card. A CVV is typically generated by the issuing bank using

a proprietary mathematical formula or algorithm at the time the ATM card is issued.

7. The CIN and CVV, together with certain other information, are sometimes referred to as "Track 2 data."

8. ATMs are typically connected to computer networks. When a customer attempts an ATM banking transaction, the Track 2 data and PIN, among other information, are transmitted over computer networks to the customer's bank for verification and authentication before the ATM transaction is allowed to proceed.

9. A magnetic stripe reader/writer ("MSR") is a device which may be used to electronically encode Track 2 data - including the CIN and CVV - onto the magnetic stripes of blank plastic ATM cards. Once so encoded, the blank plastic ATM card, together with the correct PIN, may be used to access the bank account corresponding to the Track 2 data and PIN via an ATM.

RELEVANT FINANCIAL INSTITUTIONS

At all times relevant to this Indictment, unless otherwise indicated:

Citibank

10. Citigroup Inc. was a corporation organized under the laws of the State of Delaware and headquartered in New York, New York. Citigroup Inc. provided a broad range of banking and non-banking financial services and products both within and outside of the United States. Among the subsidiaries of

Citigroup Inc. was Citibank, N.A. ("Citibank"), the deposits of which were insured by the Federal Deposit Insurance Company ("FDIC").

11. Among other things, Citibank allowed its customers to access their bank accounts, withdraw cash, and perform other activities at ATMs using Citibank-issued ATM cards and a four-digit PIN.

12. Citibank generated the CVVs - that is, the security feature encoded on its customers' ATM cards - using a proprietary algorithm. Citibank safeguarded its CVV algorithm by employing various security protocols to prevent unauthorized individuals from gaining access to it.

13. Citibank also allowed customers to access their accounts and perform banking transactions over the Internet using a website maintained by Citibank. To access an account via Citibank's website, a Citibank customer was required to enter either (1) a username and password; or (2) the bank account number, as well as the CIN and PIN associated with the account. At various times relevant to this Indictment, when a customer entered incorrect information at the website login screen, different error messages were displayed depending on the type of information that was wrong. For example, one particular error message was displayed when the correct account number or CIN, but incorrect PIN, were entered. At various times relevant to this

Indictment, when a customer entered an incorrect PIN, the Citibank website permitted the customer to attempt to enter the correct PIN a total of three times per day, for an unlimited number of days.

14. At various times relevant to this Indictment, Citibank customers were able to link together accounts to which they had access. Once a customer had linked accounts together, the customer could then transfer funds between those accounts.

15. At various times relevant to this Indictment, Citibank customers were able to reset their PINs once they had gained access to their accounts via Citibank's online banking website.

PNC Bank

16. PNC Financial Services Group Inc. was a corporation organized under the laws of the State of Pennsylvania and headquartered in Pittsburgh, Pennsylvania. PNC Financial Services Group Inc. provided a broad range of banking and non-banking financial services and products both within and outside of the United States. Among the subsidiaries of PNC Financial Services Group Inc. was PNC Bank, N.A. ("PNC Bank"), the deposits of which were insured by the FDIC.

17. PNC Bank allowed its customers to access their bank accounts and conduct transactions at ATMs and over the Internet using a website maintained by PNC Bank. To access an

account over the Internet, a PNC Bank customer was required to enter the CIN and PIN for the account, as well as the last four digits of his or her Social Security number. At various times relevant to this Indictment, the PNC Bank website allowed customers to make multiple attempts to enter the correct PIN.

THE SCHEME TO DEFRAUD

18. From at least in or about December 2005, up to and including in or about November 2008, in the Southern District of New York and elsewhere, NIKOLAY NASENKOV and ALEKSANDR KALININ, the defendants, and others known and unknown, stole bank account information from financial institutions using computer hacking and other techniques. NASENKOV, KALININ and their co-conspirators then used that account data to access the bank accounts of thousands of individual victims without authorization and without those victims' knowledge, thereby permitting NASENKOV, KALININ and others to steal millions of dollars from those accounts.

19. As a part of the fraudulent scheme, NIKOLAY NASENKOV and ALEKSANDR KALININ, the defendants, and their co-conspirators, fraudulently obtained bank account numbers, Track 2 data (including CINs and CVVs), and PINs for victims' accounts at financial institutions, including Citibank and PNC Bank.

20. As a further part of the fraudulent scheme, NIKOLAY NASENKOV and ALEKSANDR KALININ, the defendants, and their

co-conspirators, procured blank plastic ATM cards, and one or more MSRs. NASENKOV, KALININ and their co-conspirators used the MSRs to encode stolen account data onto the magnetic stripes of the blank plastic ATM cards, so that those ATM cards could be used to access individual victims' bank accounts through ATMs.

21. As a further part of the fraudulent scheme, NIKOLAY NASENKOV and ALEKSANDR KALININ, the defendants, and their co-conspirators, used fraudulently obtained PIN codes and ATM cards encoded with the stolen account data to access individual victims' accounts through ATMs located around the world, including in the United States, Estonia, Canada, Great Britain, Russia, and Turkey. After obtaining access to the victims' accounts, NASENKOV, KALININ and their co-conspirators then stole money from those accounts.

22. In some instances, and as a further part of the scheme to defraud, NIKOLAY NASENKOV, the defendant, and his co-conspirators, recruited other co-conspirators through Internet-based advertisements. Individuals who responded to the advertisements were, among other things, then provided with blank ATM cards, MSRs and stolen account data, instructed on how to encode the cards with the stolen data, and directed to withdraw money from ATMs using the ATM cards and to send those funds to NASENKOV and his co-conspirators.

23. After NIKOLAY NASENKOV and ALEKSANDR KALININ, the defendants, and their co-conspirators, had successfully stolen money from individual victims' bank accounts, they transferred the bulk of the stolen money to NASENKOV or to other co-conspirators designated by NASENKOV in Russia through various means, including through Western Union, bank wire transfers, or through one or more online digital currency exchange systems. At all times relevant to this Indictment, online digital currency exchange systems were Internet-based systems by which individuals converted cash into so-called "digital currency," which could be transferred anonymously and securely over the Internet to recipients, who then converted the digital currency into cash.

24. After NIKOLAY NASENKOV, the defendant, or others designated by NASENKOV, received the stolen money as described above, NASENKOV supplied his co-conspirators with additional stolen account data and fraudulently obtained PINs, so that his co-conspirators could again encode that additional data onto blank plastic ATM cards, and repeat the process of stealing money from victims' bank accounts through ATMs and sending NASENKOV the bulk of the proceeds.

2006 PNC BANK ATTACK

25. As part of the scheme to defraud, from on or about January 16, 2006, up to and including on or about January 20, 2006, an attack by one or more hackers was launched against PNC

Bank's online banking website. The attack, which exploited the fact that PNC Bank's website allowed customers to make multiple attempts to enter the correct PIN for a particular account, used a computer program to make thousands of attempts to guess the correct PINs for certain PNC Bank accounts. The PINs for hundreds of PNC Bank customer accounts were compromised during this attack.

26. NIKOLAY NASENKOV, the defendant, supplied Track 2 data and PINs from the PNC Bank accounts compromised as a result of the attack to co-conspirators, who encoded blank plastic ATM cards with the data and used the ATM cards to withdraw approximately $1.3 million from victims' accounts via ATMs around the world, including in Estonia.

27. After withdrawing the money, the co-conspirators of NIKOLAY NASENKOV, the defendant, sent NASENKOV or others designated by NASENKOV the bulk of the cash.

2007 CITIBANK ATM DATA BREACH

28. As part of the scheme to defraud, from in or about October 2007, up to and including in or about November 2007, ALEKSANDR KALININ, the defendant, and others known and unknown, placed a "sniffer" program on a computer network that processed ATM transactions for Citibank and other financial institutions. At all times relevant to this Indictment, a "sniffer" program was a piece of malicious computer code that, among other things,

surreptitiously recorded data passing over a computer network including, for example, Track 2 data and PINs, and exported that data to an outside computer. Through the use of this malicious computer code, KALININ stole Track 2 data and encrypted PINs for approximately 500,000 bank accounts, including approximately 100,000 Citibank accounts.

29. NIKOLAY NASENKOV, the defendant, obtained this account information that ALEKSANDR KALININ, the defendant, had stolen. NASENKOV then supplied Track 2 data and decrypted PINs from the Citibank accounts compromised as a result of the data breach perpetrated by KALININ, and others, to co-conspirators, who encoded blank plastic ATM cards and used them to withdraw approximately $2.9 million from Citibank customers' accounts via ATMs around the world, including in New York, New York.

30. After withdrawing the money, the co-conspirators of NIKOLAY NASENKOV AND ALEKSANDR KALININ, the defendants, sent the bulk of the cash to NASENKOV or to others designated by NASENKOV.

2008 CITIBANK ATTACK

31. From in or about July 2008, up to and including in or about November 2008, NIKOLAY NASENKOV, the defendant, used a computer program (the "Attack Program") to mount an attack against Citibank's online banking website. The computer program, which exploited the fact that customers could make up to three

attempts per day to enter the correct PIN for a particular account, made hundreds of thousands of attempts to guess the correct PINs for hundreds of thousands of Citibank customers' accounts. For example, from on or about August 24, 2008 through on or about August 25, 2008, the Attack Program made over 600,0000 unsuccessful attempts to access Citibank customers' accounts and over 300,000 successful attempts to access Citibank customers' accounts.

32. Among other things, the Attack Program used by NIKOLAY NASENKOV, the defendant, generated sequential Citibank CINs. Then, NASENKOV's Attack Program made multiple attempts to guess the correct PIN for each CIN. Once NASENKOV's Attack Program detected a correct CIN and PIN combination based on the messages (including the error messages) supplied by Citibank's online banking website, it accessed the customer's account and then reset the PIN to a particular value. The Attack Program also attempted to link the particular compromised account to other compromised accounts, and if successful, attempted to transfer funds between the compromised accounts. NASENKOV's Attack Program then generated Track 2 data for the compromised accounts. In generating the Track 2 data, NASENKOV's Attack Program used an algorithm to generate CVVs.

33. NASENKOV supplied Track 2 data and PINs relating to the Citibank accounts compromised as a result of the Attack

Program to co-conspirators, who used the information to encode blank plastic ATM cards and then to withdraw approximately $3.6 million from Citibank customers' accounts via ATMs around the world, including in Tallinn, Estonia and New York, New York.

34. After withdrawing the money through this scheme to defraud, the co-conspirators of NIKOLAY NASENKOV, the defendant, sent NASENKOV or others designated by NASENKOV the bulk of the cash.

STATUTORY ALLEGATIONS

35. From at least in or about December 2005, up to and including in about November 2008, in the Southern District of New York and elsewhere, NIKOLAY NASENKOV and ALEKSANDR KALININ, the defendants, and others known and unknown, unlawfully, willfully, and knowingly did combine, conspire, confederate, and agree together and with each other to commit an offense against the United States, to wit, to violate Title 18, United States Code, Section 1344.

36. It was a part and an object of the conspiracy that NIKOLAY NASENKOV and ALEKSANDR KALININ, the defendants, and others known and unknown, unlawfully, willfully, and knowingly would and did execute and attempt to execute a scheme and artifice to defraud financial institutions, the deposits of which were then insured by the Federal Deposit Insurance Corporation, and to obtain monies, funds, credits, assets, securities, and

other property owned by and under the custody and control of such financial institutions, by means of false and fraudulent pretenses, representations, and promises, in violation of Title 18, United States Code, Section 1344.

OVERT ACTS

37. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about December 9, 2005, NIKOLAY NASENKOV, the defendant, posted an advertisement on the Internet seeking individuals to withdraw money from ATMs in the United States using blank ATM cards encoded with stolen Track 2 data and PINs.

b. In or about January 2006, NIKOLAY NASENKOV, the defendant, obtained bank account data for hundreds of individual victims' accounts at PNC Bank.

c. On or about January 13, 2006, NIKOLAY NASENKOV, the defendant, exchanged instant messages over the Internet with a co-conspirator in Estonia not named as a defendant herein ("CC-1"). During the exchange, in sum and substance, NASENKOV and CC-1 acknowledged that they had conspired together before to withdraw money from bank accounts via ATMs using stolen account information. In addition, NASENKOV informed

CC-1 that he had Track 2 data and PINs for accounts at a new bank, that the Track 2 data and PINs had been successfully tested in the United States, and that approximately $1,000 could be withdrawn from each account.

d. In or about January 2006, NIKOLAY NASENKOV, the defendant, emailed to CC-1 Track 2 data and PINs for five PNC Bank accounts so that CC-1 and his co-conspirators could encode blank ATM cards and withdraw money from ATMs in Estonia.

e. In or about January 2006, CC-1 and his co-conspirators used the stolen account information from NIKOLAY NASENKOV, the defendant, to withdraw approximately $3,800 from approximately five PNC Bank customers' accounts.

f. In or about January 2006, CC-1 sent NIKOLAY NASENKOV, the defendant, an instant message reporting the amount of cash that CC-1 and his co-conspirators had withdrawn from each of the five PNC Bank accounts referred to above.

g. In or about January 2006, NIKOLAY NASENKOV, the defendant, sent CC-1 a list of names of individuals in St. Petersburg, Russia to whom CC-1 should send NASENKOV's share of the cash by Western Union.

h. From at least in or about October 2007, up to and including in or about November 2007, ALEKSANDR KALININ, the defendant, installed a sniffer program on a computer network that processed ATM transactions for various banks, including Citibank,

which program stole and exported account information for thousands of Citibank customers' accounts to KALININ and others.

i. From at least in or about October 2007, up to and including in or about February 2008, NIKOLAY NASENKOV, the defendant, obtained bank account data for thousands of individual victims' accounts at Citibank that had been stolen by the sniffer program.

j. In or about December 2007, NASENKOV e-mailed to a co-conspirator in Estonia not named as a defendant herein ("CC-2"), Track 2 data and PINs pertaining to the accounts of multiple Citibank customers.

k. In or about December 2007, CC-2 emailed to a co-conspirator in Michigan not named as a defendant herein ("CC-3") stolen account data that he had received from NIKOLAY NASENKOV, the defendant, pertaining to the accounts of multiple Citibank customers, and sent to CC-3 a number of blank plastic ATM cards and an MSR, so that CC-3 could encode the blank ATM cards with the stolen account data.

l. On or about January 12, 2008, CC-3, while in New York, New York, used blank ATM cards encoded with stolen account information to withdraw a total of approximately $2,000 from a Citibank customer's account.

m. From in or about December 2007, up to and including in or about February 2008, NIKOLAY NASENKOV, the

defendant, e-mailed to a co-conspirator in New York, New York not named as a defendant herein ("CC-4"), stolen account information pertaining to multiple Citibank customers' accounts, so that CC-4 could encode blank ATM cards with the stolen account data and withdraw money from ATMs located in New York, New York.

n. On or about February 14, 2008, CC-4 used an ATM card encoded with stolen account information at an ATM in New York, New York, to withdraw approximately $2,350 from a Citibank customer's account.

o. On or about February 20, 2008, CC-4 transferred approximately $40,453 to NIKOLAY NASENKOV, the defendant, via WebMoney, an online digital currency exchange system.

p. On or about February 21, 2008, CC-4 and another co-conspirator not named as a defendant herein ("CC-5") used an ATM card encoded with stolen account information at an ATM in New York, New York, to withdraw approximately $4,000 from a Citibank customer's account.

q. On or about February 24, 2008, CC-4 transferred approximately $34,500 to NIKOLAY NASENKOV, the defendant, via WebMoney.

r. From in or about July 2008, up to and including at least in or about November 2008, NIKOLAY NASENKOV, the defendant, used the Attack Program to obtain bank account data for thousands of victims' accounts at Citibank.

s. On or about July 24, 2008, NIKOLAY NASENKOV, the defendant, sent to CC-4 stolen account data for 11 Citibank customers' accounts via e-mail and, in the email, NASENKOV informed CC-4 that the account information came from a "new database."

t. On or about August 10, 2008, NIKOLAY NASENKOV, the defendant, contacted a co-conspirator in Estonia not named as a defendant herein ("CC-6") via ICQ, an instant message service. In sum and substance, NASENKOV offered to provide CC-6 with stolen account data for hundreds of individual victims' accounts at Citibank, which CC-6 would then use to encode blank ATM cards and steal money from individual Citibank customers' accounts via ATM machines in Estonia and elsewhere. NASENKOV and CC-6 agreed that CC-6 would cause 70% of the funds to be sent to NASENKOV outside of Estonia via WebMoney.

u. On or about August 10, 2008, NIKOLAY NASENKOV, the defendant, sent CC-6 stolen account information for approximately 150 Citibank customers' accounts via e-mail.

v. On or about August 10, 2008, CC-6 used ATM cards encoded with the stolen account information that he had received from NIKOLAY NASENKOV, the defendant, to withdraw a total of at least $15,730 from Citibank customers' accounts and then transferred at least $6,000 of that money to NASENKOV via WebMoney.

w. On or about August 11, 2008, NIKOLAY NASENKOV, the defendant, sent CC-6 stolen account information for several hundred additional individual Citibank customers' accounts via e-mail.

x. On or about August 27, 2008, NIKOLAY NASENKOV, the defendant, transferred a file which comprised part of the Attack Program from a computer located in Russia to a computer server located in California (the "California Server").

y. On or about October 20, 2008, NIKOLAY NASENKOV, the defendant, accessed files which comprised part of the Attack Program on the California server from a computer in Russia.

z. On or about October 23, 2008, NIKOLAY NASENKOV, the defendant, transferred files which comprised part of the Attack Program to the California Server.

aa. On or about October 24, 2008, NIKOLAY NASENKOV, the defendant, logged onto the California Server and accessed a list of files related to the Attack Program.

ab. On or about October 27, 2008, NIKOLAY NASENKOV, the defendant, exchanged ICQ messages with a co-conspirator in the United States not named as a defendant herein ("CC-7"). During the exchange, in sum and substance, NASENKOV inquired if CC-7 was prepared to encode ATM cards with stolen

account information and withdraw money from victims' bank accounts via ATMs.

(Title 18, United States Code, Section 1349.)

COUNTS TWO THROUGH FIVE

(Bank Fraud)

The Grand Jury further charges:

38. The allegations in paragraphs 1 through 35 and 38 are repeated, re-alleged and reincorporated as if set forth fully herein.

39. On or about the dates set forth below, in the Southern District of New York and elsewhere, NIKOLAY NASENKOV and ALEKSANDR KALININ, the defendants, and others known and unknown, unlawfully, willfully, and knowingly did execute and attempt to execute a scheme and artifice to defraud a financial institution, the deposits of which were then insured by the Federal Deposit Insurance Corporation, and to obtain monies, funds, credits, assets, securities, and other property owned by and under the custody and control of such financial institution by means of false and fraudulent pretenses, representations, and promises, to wit, NASENKOV, KALININ and others known and unknown fraudulently withdrew the amount of funds listed below from the accounts of Citibank customers via ATMs at the locations listed below using ATM cards encoded with stolen account information:

COUNT	APPROX. DATE	WITHDRAWAL
TWO	January 12, 2008	Approximately $2,000 by CC-3 via an ATM in New York, New York.
THREE	February 14, 2008	Approximately $2,350 by CC-4 via an ATM in New York, New York.
FOUR	February 21, 2008	Approximately $4,000 by CC-4 and CC-5 via an ATM in New York, New York.
FIVE	August 10, 2008	Approximately $15,730 by CC-6 via ATMs in Tallinn, Estonia.

(Title 18, United States Code, Sections 1344 and 2.)

COUNT SIX

(Conspiracy to Commit Access Device Fraud)

The Grand Jury further charges:

40. The allegations in paragraphs 1 through 35 and 38 are repeated, re-alleged and reincorporated as if set forth fully herein.

41. From at least in or about December 2005, up to and including in or about November 2008, in the Southern District of New York and elsewhere, NIKOLAY NASENKOV and ALEKSANDR KALININ, the defendants, and others known and unknown, unlawfully, willfully, and knowingly did combine, conspire, confederate, and agree together and with each other to commit an offense against the United States, to wit, to violate Title 18, United States Code, Sections 1029(a)(2), 1029(a)(3), and 1029(a)(5).

42. It was a part and an object of the conspiracy that NIKOLAY NASENKOV and ALEKSANDR KALININ, the defendants, and

others known and unknown, unlawfully, willfully and knowingly, and with intent to defraud, in an offense affecting interstate and foreign commerce, would and did traffic in and use one and more unauthorized access devices during a one year period, and by such conduct would and did obtain a thing of value aggregating $1,000 and more during that period, in violation of Title 18, United States Code, Section 1029(a)(2).

43. It was further a part and an object of the conspiracy that NIKOLAY NASENKOV and ALEKSANDR KALININ, the defendants, and others known and unknown, unlawfully, willfully and knowingly, and with intent to defraud, in an offense affecting interstate and foreign commerce, would and did possess fifteen and more devices which were counterfeit and unauthorized access devices, in violation of Title 18, United States Code, Section 1029(a)(3).

44. It was further a part and an object of the conspiracy that NIKOLAY NASENKOV and ALEKSANDR KALININ, the defendants, and others known and unknown, unlawfully, willfully and knowingly, and with intent to defraud, in an offense affecting interstate and foreign commerce, would and did effect transactions, with one and more access devices issued to another person and persons, to receive payment and another thing of value during a one-year period the aggregate value of which was equal to or greater than $1,000, in violation of Title 18, United States Code, Section 1029(a)(5).

OVERT ACTS

45. In furtherance of the conspiracy and to effect the illegal objects thereof, the overt acts described above in paragraph 38 were committed in the Southern District of New York and elsewhere.

(Title 18, United States Code, Section 1029(b)(2).)

COUNT SEVEN

(Computer Intrusion Obtaining Information)

The Grand Jury further charges:

46. The allegations in paragraphs 1 through 35 and 38 are repeated, re-alleged and reincorporated as if set forth fully herein.

47. From at least in or about July 2008, up to and including in or about November 2008, in the Southern District of New York and elsewhere, NIKOLAY NASENKOV, the defendant, for purposes of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, intentionally accessed and attempted to access a computer without authorization, and thereby obtained and attempted to obtain information contained in a financial record of a financial institution, and of a card issuer as defined in 15 U.S.C. § 1602(n), and from a protected computer, the value of which exceeded $5,000, to wit, using the Attack Program, NASENKOV

accessed and attempted to access without authorization a computer network maintained by or for the benefit of Citibank, and thereby obtained and attempted to obtain account information relating to thousands of Citibank customers' accounts, which information was used to fraudulently withdraw millions of dollars from those accounts.

(Title 18, United States Code,
Sections 1030(a)(2), 1030(b), 1030(c)(2)(B)(i)-(iii), and 2.)

COUNT EIGHT

(Computer Intrusion Furthering Fraud)

The Grand Jury further charges:

48. The allegations in paragraphs 1 through 35 and 38 are repeated, re-alleged and reincorporated as if set forth fully herein.

49. From at least in or about July 2008, up to and including in or about November 2008, in the Southern District of New York and elsewhere, NIKOLAY NASENKOV, the defendant, knowingly and with intent to defraud, accessed and attempted to access a protected computer without authorization, and by means of such conduct furthered the intended fraud and obtained something of value exceeding $5,000, to wit, using the Attack Program, NASENKOV accessed and attempted to access without authorization a computer network maintained by or for the benefit of Citibank, and thereby obtained and attempted to obtain account information relating to thousands of Citibank customers'

accounts, which information was used to fraudulently withdraw millions of dollars from those accounts.

(Title 18, United States Code,
Sections 1030(a)(4), 1030(b), 1030(c)(3)(A), and 2.)

COUNT NINE

(Aggravated Identity Theft)

The Grand Jury further charges:

50. The allegations in paragraphs 1 through 35 and 38 are repeated, re-alleged and reincorporated as if set forth fully herein.

51. From at least in or about December 2005, up to and including in or about November 2008, in the Southern District of New York and elsewhere, NIKOLAY NASENKOV and ALEKSANDR KALININ, the defendants, unlawfully, willfully, and knowingly did transfer, possess, and use, without lawful authority, a means of identification of another person, during and in relation to the felony violation charged in Count One of this Indictment, to wit, NASENKOV and KALININ possessed and used CINs and PINs for Citibank customers and transferred those CINs and PINs to others to fraudulently withdraw money from those Citibank customers' accounts via ATMs.

(Title 18, United States Code,
Sections 1028A(a)(1), 1028A(b), and 2.)

COUNT TEN

(Conspiracy to Commit Money Laundering)

The Grand Jury further charges:

52. The allegations in paragraphs 1 through 35 and 38 are repeated, re-alleged and reincorporated as if set forth fully herein.

53. From at least in or about December 2005, up to and including in or about November 2008, in the Southern District of New York and elsewhere, NIKOLAY NASENKOV, the defendant, and others known and unknown, unlawfully, willfully, and knowingly did combine, conspire, confederate, and agree together and with each other to commit offenses against the United States, to wit, to violate Title 18, United States Code, Sections 1956(a)(1)(A)(i) and 1956(a)(1)(B)(i).

54. It was a part and an object of the conspiracy that NIKOLAY NASENKOV, the defendant, and others known and unknown, in an offense involving and affecting interstate and foreign commerce, knowing that the property involved in financial transactions represented the proceeds of some form of unlawful activity, unlawfully, willfully and knowingly, would and did conduct and attempt to conduct such financial transactions which in fact involved the proceeds of specified unlawful activity, to wit, access device fraud and bank fraud, with the intent to promote the carrying on of specified unlawful activity, in

violation of Title 18, United States Code, Section 1956(a)(1)(A)(i).

55. It was further a part and an object of the conspiracy that NIKOLAY NASENKOV, the defendant, and others known and unknown, in an offense involving and affecting interstate and foreign commerce, knowing that the property involved in financial transactions represented the proceeds of some form of unlawful activity, unlawfully, willfully and knowingly, would and did conduct and attempt to conduct such financial transactions which in fact involved the proceeds of specified unlawful activity, to wit, access device fraud and bank fraud, knowing that the transactions were designed in whole and in part to conceal and disguise the nature, the location, the source, the ownership, and the control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

OVERT ACTS

56. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about February 9, 2008, CC-4 transferred approximately $68,000 from a location in the Southern District of New York to NIKOLAY NASENKOV, the defendant, via WebMoney.

b. On or about February 11, 2008, CC-4 transferred approximately $50,000 from a location in the Southern District of New York to NIKOLAY NASENKOV, the defendant, via WebMoney.

c. On or about February 20, 2008, CC-4 transferred approximately $40,453 from a location in the Southern District of New York to NIKOLAY NASENKOV, the defendant, via WebMoney.

d. On or about February 24, 2008, CC-4 transferred approximately $34,500 from a location in the Southern District of New York to NIKOLAY NASENKOV, the defendant, via WebMoney.

(Title 18, United States Code, Section 1956(h).)

COUNT ELEVEN

(Conspiracy to Commit Computer Intrusion)

The Grand Jury further charges:

57. The allegations in paragraphs 1 through 35 and 38 are repeated, re-alleged and reincorporated as if set forth fully herein.

58. From at least in or about October 2007, up to and including in or about February 2008, in the Southern District of New York and elsewhere, NIKOLAY NASENKOV and ALEKSANDR KALININ, the defendants, and others known and unknown, unlawfully, willfully, and knowingly did combine, conspire, confederate, and agree together and with each other to commit an offense against

the United States, to wit, to violate Title 18, United States Code, Sections 1030(a)(2), 1030(a)(4).

59. It was a part and an object of the conspiracy that NIKOLAY NASENKOV and ALEKSANDR KALININ, the defendants, and others known and unknown, unlawfully, willfully and knowingly, for purposes of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, intentionally accessed a computer without authorization, and thereby obtained and attempted to obtain information contained in a financial record of a financial institution, and of a card issuer as defined in 15 U.S.C. § 1602(n), and from a protected computer, the value of which exceeded $5,000, in violation of Title 18, United States Code, Section 1030(a)(2).

60. It was further a part and an object of the conspiracy that NIKOLAY NASENKOV and ALEKSANDR KALININ, the defendants, and others known and unknown, knowingly and with intent to defraud, accessed and attempted to access a protected computer without authorization, and by means of such conduct furthered the intended fraud and obtained something of value exceeding $5,000, in violation of Title 18, United States Code, Section 1030(a)(4).

OVERT ACTS

61. In furtherance of the conspiracy and to effect the illegal objects thereof, the overt acts described above in

paragraph 38 were committed in the Southern District of New York and elsewhere.

(Title 18, United States Code, Section 1030(b)(2).)

FORFEITURE ALLEGATION

(As to Counts One though Five, Seven, Eight and Eleven)

62. As a result of committing one or more of the bank fraud or computer intrusion offenses alleged in Counts One through Five, Seven, Eight and Eleven, NIKOLAY NASENKOV, the defendant; and as a result of committing one or more of the bank fraud or computer intrusion offenses alleged in Counts One through Five and Eleven, ALEKSANDR KALININ, the defendant, shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(2), any property constituting, or derived from, proceeds obtained directly or indirectly as a result of such violation, including but not limited to the following:

a. At least approximately $7.8 million in United States currency, in that such sum in aggregate is property representing the amount of proceeds obtained as a result of the offenses.

Substitute Assets Provision

63. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States, pursuant to 18 U.S.C. § 982(b), to seek forfeiture of any other property of said defendant up to the value of the above-described forfeitable property.

(Title 18, United States Code, Sections 982, 1344 and 1349.)

FORFEITURE ALLEGATION

(As to Count Six)

64. As a result of committing the access device fraud offense alleged in Count Six, NIKOLAY NASENKOV and ALEKSANDR KALININ, the defendants, shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(2)(B), any property constituting, or derived from, proceeds obtained directly or indirectly as a result of such violation, and pursuant to 18 U.S.C. § 1029(c), any personal property used or intended to be used to commit the offense, including but not limited to the following:

a. At least approximately $7.8 million in United States currency, in that such sum in aggregate is property

representing the amount of proceeds obtained as a result of the offense alleged in Count One.

Substitute Assets Provision

65. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States, pursuant to 18 U.S.C. § 982(b), to seek forfeiture of any other property of said defendant up to the value of the above-described forfeitable property.

(Title 18, United States Code, Sections 982 and 1029.)

FORFEITURE ALLEGATION

(As to Count Ten)

66. As a result of committing the money laundering offense alleged in Count Ten, NIKOLAY NASENKOV, the defendant, shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(1), all property, real and personal, involved in such offense and all property traceable to such property, including but not limited to the following:

a. At least approximately $7.8 million in United States currency, in that such sum in aggregate is property which was involved in the money laundering offense or is traceable to such property.

Substitute Assets Provision

67. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States, pursuant to 18 U.S.C. § 982(b), to seek forfeiture of any other property of said defendant up to the value of the above-described forfeitable property.

(Title 18, United States Code, Sections 982 and 1956.)

[redacted]
FOREPERSON

PREET BHARARA
United States Attorney JK